zdf.de

Sicherheitslücke in Software: Citrix: Gesetz ermöglicht Schwachstellen

10-12 minutes

Derzeit laufen massive Angriffe auf Zugriffsgateways des Software-Herstellers Citrix. Um nun Sicherheitslücken in Betrieben und Behörden schnell zu beseitigen, fehlen Gesetze.

Sicherheitslücke bei Citrix (Archiv): Auch Feuerwehren und Polizeien arbeiten mit dem System.

Quelle: Imago

Die Sicherheitslücke in der Fernzugriffssoftware Citrix ist schon seit einigen Wochen bekannt. Inzwischen gibt es

auch Schadsoftware, die diese Sicherheitslücke ausnutzt, um lokale Netze zu infiltrieren. Doch ein entsprechendes Sicherheitsupdate, um die Lücke zu schließen, wird noch ein bis zwei Wochen auf sich warten lassen.

Dabei kann durch die Sicherheitslücke Schadsoftware auf die Anwendungen der Citrix-Kunden gelangen. Die Folgen reichen von Spionage bis hin zur Abschaltung der Systeme.

Rettungsleitstellen sind bedroht

Die Folgen sind derzeit noch nicht abzusehen. Denn die Citrix-Software wird von vielen Unternehmen und Behörden eingesetzt, damit deren Mitarbeiter von zu Hause oder auf Dienstreisen auf ihren Computerarbeitsplatz im Büro zugreifen können und mit derselben IT-Umgebung arbeiten wie im Büro.

Die Sicherheitslücke wurde am 23. Dezember 2019 veröffentlicht. Hersteller Citrix reagierte noch Heiligabend darauf und empfahl Anwendern eine Übergangslösung, bis ein Sicherheitsupdate Ende Januar 2020 verfügbar sein würde. Daraufhin gingen offenbar alle in die Weihnachtsferien.

Das Bundesamt für Sicherheit in der Informationstechnik veröffentlichte eine entsprechende Warnmeldung erst ab dem 7. Januar. Inoffiziell war von IT-Sicherheitsspezialisten, die für Bundesbehörden arbeiten, zu hören, dass während der Weihnachtsferien ohnehin nicht gearbeitet würde.

Keine Sicherheit während der Feiertage

Tatsächlich war bei den meisten Citrix-Anwendern während der Feiertage Betriebsruhe angesagt, aber eben nicht bei allen. Denn neben Baumärkten, Automobilfabriken oder

Steuerämtern, deren Beschäftigte unterm Weihnachtsbaum saßen, setzen auch Leitstellen der Polizei, der Rettungsdienst der Feuerwehren, Kliniken und Stadtwerke die Citrix-Fernzugriffssoftware ein.

Dort wurde auch über Weihnachten gearbeitet. Und diese Stellen gelten als Betreiber sogenannter kritischer Infrastrukturen. Legt ein Hackerangriff zum Beispiel eine Rettungsleitstelle, ein Krankenhaus oder ein Wasserwerk lahm, hat das massive Auswirkungen. "Der Angriff ist vergleichsweise einfach und entsprechende Angriffswerkzeuge bereits frei verfügbar", warnte die AG Kritis, eine Arbeitsgemeinschaft von IT-Sicherheitsexperten, die sich um kritische Infrastrukturen kümmern, bereits am vergangenen Wochenende.

Dabei hätte die Citrix-Sicherheitslücke längst geschlossen werden müssen. Bereits seit Jahren fordern namhafte Sicherheitsexperten eine Meldepflicht für Sicherheitslücken. "Nur wenn gesetzlich geregelt ist, dass eine Sicherheitslücke gemeldet, sobald sie bekannt wird, und dann in Zusammenarbeit mit den zuständigen Behörden beseitigt werden muss, werden wir das notwendige IT-Sicherheitsniveau erreichen", begründet Informatik-

Professor Hartmut Pohl die Einführung einer solchen Meldepflicht.

Seehofer wollte die Meldepflicht

Die regierungsnahe Stiftung Neue Verantwortung hatte im Jahr 2018 sogar schon ein Konzept für eine solche Meldepflicht ausgearbeitet. Bundesinnenminister Horst Seehofer wollte die Meldepflicht für Sicherheitslücken in das IT-Sicherheitsgesetz 2.0 einbringen. Seinen Beamten im Innenministerium hatte Seehofer auf dem Digitalgipfel der Bundesregierung Anfang Dezember 2018 in Nürnberg deshalb auch schon angekündigt: "Sie kriegen jetzt jede Woche die Frage: Wo ist die Meldepflicht?"

Doch bei den konkreten Beratungen zum zweiten IT-Sicherheitsgesetz war die Sicherheitslücken-Meldepflicht dann kein Thema mehr. Die Sicherheitsbehörden und Militärs hatten sich durchgesetzt. Sie brauchen derartige Sicherheitslücken, damit ihre digitalem Angriffswaffen und ihre Spionagesoftware funktioniert. Deshalb werden Sicherheitslücken bewusst offengehalten. Und deshalb gibt es bisher keine Meldepflicht für solche Sicherheitslücken. Für die IT-Sicherheit hat das massive Konsequenzen.

Nachrichtendienstliche Lobby hat sich durchgesetzt

Seit Jahren bestehende Sicherheitslücken in Kraftwerken können jederzeit von Online-Kriminellen genutzt werden, um Deutschland flächendeckend den Strom abzuschalten. Krankenhäuser mussten sich tagelang von der Notfallversorgung abmelden. Die Ursache: Angreifer hatten schon lange bekannte Sicherheitslücken ausgenutzt, die trotz ihres Bekanntheitsgrades immer noch nicht beseitigt

waren. Auch an Hochschulen in Berlin, Freiburg und Gießen richteten offene und lange bekannte Sicherheitslücken Schäden an.

Doch sowohl die Warnungen als auch die Kassandrarufe der IT-Sicherheitsexperten sind bisher von der Bundesregierung ignoriert worden.